SECURE AUTHENTICATION FOR BUSINESS MANAGEMENT SYSTEM USING COLOR PASS

*Barkha Patel [1] | Keval Shah [1] | Kevan Godhani [1]

[1] Student, Computer, Sinhgad College of Engineering, Pune, India - 411041. (*Corresponding Author)

ABSTRACT

Security in Business Management System is an important aspect in maintaining confidentiality of company's essential data. Thereby, a more secure authentication scheme is required. Classical PIN entry mechanism is widely used for authenticating a user. It is a popular scheme because it nicely balances the usability and security aspects of a system. However, this scheme may suffer from shoulder surfing attack. In this attack, an unauthorized user can fully or partially observe the login session. Even the activities of the login session can be recorded which the attacker can use it later to get the actual PIN. We propose an intelligent user interface, known as Color Pass to resist the shoulder surfing attack so that any genuine user can enter the session PIN without disclosing the actual PIN. The Color Pass is based on a partially observable attacker model. The experimental analysis shows that the Color Pass interface is safe and easy to use even for novice users.

KEYWORDS: Color PIN, Shoulder Surfing Attack, Password, Partially Observable, Board Of Directors.

Introduction

In computer security, authentication is such a technique by which the system identifies the genuine users. Among several authentication schemes, password based authentication is still one of the widely accepted solution for its ease of use and cost effectiveness. Though conventional PIN entry mechanism is widely famous for ease of usability, but it is prone to shoulder surfing attack in which an attacker can record the login procedure of a user for an entire session and can retrieve the user original PIN.

Based on the information available to the attacker, secure login methods can be classified into two broad categories fully observable and partially observable. In the first one, the attacker can fully observe the entire login procedure for a particular session and in the second one, the attacker can partially observe the login procedure. Our proposed methodology falls into second category and users are required to remember four colors instead of conventional four digit PINs.

The proposed Color Pass methodology implements onetime pass paradigm. Thus corresponding to four color PINs, the user gets four challenges and enters four responses with respect to each challenge. The main objective of Color Pass scheme is that it is easy to use and does not require any special prerequisite knowledge. In addition to the resistance against shoulder surfing attack, it also provides equal password strength as compared with the conventional PIN entry scheme.

Materials and Methods:

A. *Characteristic of user chosen PIN*

In the conventional schemes it is required to remember either few digits or characters as user PIN. But in our scheme colors are used to form a PIN. User can choose four colors from a set of ten different colors represented as $\{C_0, C_1, \cdots, C_9\}$. User has the flexibility to choose one color more than once, like $C_1C_5C_1C_4$. As user chosen PIN is comprised of four colors so probability of guessing the PIN will be $1/10^4$.

B. *Steps of Login Procedure*

In this subsection we will discuss about user's interaction with system during entire session.

- User enters his login id.
- Once system checks that the login id exists then it will generate Feature Tables using Algorithm 1.
- System then generates four random challenge values ranges from $0 \cdots 9$.
- Next user will have to give response to those challenge values.
- User response will be evaluated by system using Algorithm 2.
- Finally system will decide whether the user is legitimate or not using Algorithm 3.

C. *Characteristic of Feature Tables*

Color Pass interface consists of 10 different Feature Tables which are numbered from 0 to 9. Each cell of a table is represented by pair $< C_i, V_i >$. Here C_i is the color of the cell i and V_i indicates the digit corresponding to cell i. The pair $< C_i, V_i >$ is unique with respect to all the cells in all the ten tables.

D. *Algorithm for Generating Tables*

Suppose ten different colors $\{C_0, C_2,...,C_9\}$ are stored in an array Color[ ]. This array is required as an input to Algorithm 1. Now let's assume that each Feature Table is denoted as FT (i) and each cell is by CELL (j). So to refer a cell of a table we use an operator FT(i).CELL(j).

By using Algorithm 1, all the cells of ten Feature Tables will be initialized with some unique color and value combination.

Algorithm 1 Generating tables in Color Pass

```
Input: This algorithm will take array Color [0,1,...9] as input.
Output: It will generate Feature Tables F T (0) · · ·
F T (9) for i = 0 to 9 do
for j = 0 to 9 do
FT(i).CELL(j).Color ← Color[j]
FT(i).CELL(j).Value ← (i+j) mod 10;
end for
end for
```

E. *PIN Entry Mechanism in Color Pass*

In this scheme, the user chosen PIN is four colors and a pattern to get challenge values. If user selects Pattern 1, then the challenge values are last 4 digits of a randomly generated 10 digit number. In Pattern 2 first 4 digits are challenge values and in Pattern 3 first 2 digits and last 2 digits are the challenge values. During the login procedure, when the Feature Tables appear on the screen then the system throws challenge values to the user.

Challenge values range from 0 to 9. Based on the challenge value the user has to select the corresponding Feature Table. For example, challenge value 4 indicates that the user has to look in the Fourth Feature Table. The challenge values will be generated using psudo random function. User will receive challenge corresponding to each color of his PIN. Then corresponding to the chosen color PIN, he locates the color cell in that table. The user then finds the value of that color cell and enters that digit as response to the challenge. Similarly user will respond to the other three challenge values and will complete the login process. Valid response to the challenge values will authenticate the user. Methodology of evaluating user successfully response is given below.

We have stored user PIN in an array UCOL and challenge values generated by system has been stored in array RAN. User response to the challenge has been stored in array CLICK. Array EVAL has been initialized by 0 initially and valid holds the correct response value for each challenge. All these arrays have been used for implementing Algorithm 2.

Algorithm 2 Evaluating User Response in Color Pass

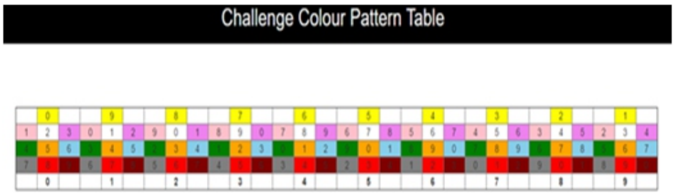
```
Input: This algorithm will take array UCOL, array CLICK and array RAN
as input.
Output: This algorithm will update value of array
EVAL by 1 for each valid response.
for i = 0 to 3 do
K ← RAN[i] − 1
Valid ← (UCOL[i] + K) mod 10 if CLICK[i] := Valid then
EVAL[i] ← 1
end if
end for
```

Algorithm 3 User Authentication

```
Input: This algorithm will take array EVAL as input after executing
Algorithm 2.
Output: Decides whether user is allowed to Login.
Initialize X := 0 for i = 0 to 3 do
if EVAL[i] := 1 then
X ← 1 else
X ← 0 break
end if end for
if X := 1 then
Allow user to Login else
Disallow the user end if
```

F. ***User Interface for Color Pass***

Ten colors are chosen in such a way that each color is clearly distinguishable from other. The actual interface is shown in Fig. 1. As the color cell's position in each table is fixed so user can locate the desired colored cell quite quickly.



Challenge Colour Pattern Table

	0			9			8			7			6			5			4			3			2			1	
1	2	3	0	1	2	9	0	1	8	9	0	7	8	9	6	7	8	5	6	7	4	5	6	3	4	5	2	3	4
4	5	6	3	4	5	2	3	4	1	2	3	0	1	2	9	0	1	8	9	0	7	8	9	6	7	8	5	6	7
7	8	9	6	7	8	5	6	7	4	5	6	3	4	5	2	3	4	1	2	3	0	1	2	9	0	1	8	9	0
	0			1			2			3			4			5			6			7			8			9	

Fig. 1: User Interface on Screen

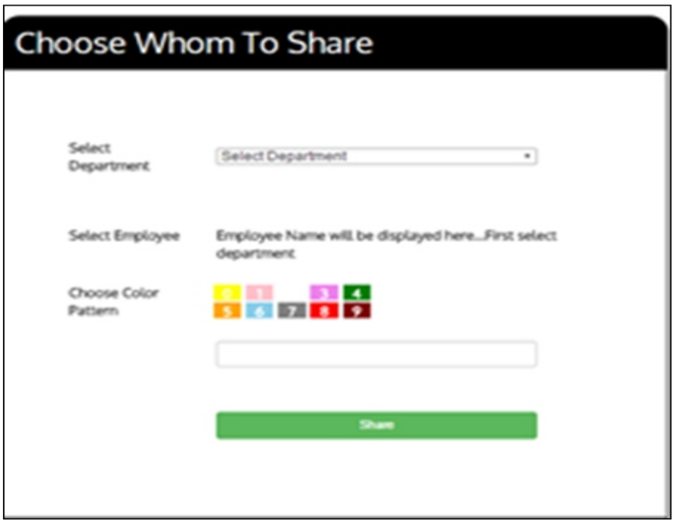
G. ***Color Pass in Business Management System***

1. User login

While registration user choses a color PIN and a Pattern. During the login procedure, Feature Tables and challenge values appear on the screen.

2. Employee Login

Employee login is similar to user login. An employee after login can update profile, upload files, share files to another employee with a secure color PIN, check shared history, and download files.



Choose Whom To Share

Select Department: Select Department

Select Employee: Employee Name will be displayed here...First select department

Choose Color Pattern: 0 1 3 4 / 5 6 7 8 9

Fig. 2: File sharing with color PIN

When an employee shares a file, the other employee will receive a notification about the shared file and will also get a PIN to unlock and download that file.

3. Directors login

In proposed Business Management System, only Board Of Directors can access company's confidential data. All the Board Of Directors have to enter their password as per predefined sequence before the system timeout. Our system has maximum five BODs. Admin can add/remove BODs and can also assign priority.

Results and Discussion:

In this scheme, the user remembers four colors as his PIN. The scheme works on the framework of partially observable attacker model. From security point of view the scheme is quite robust against shoulder surfing, guessing password. From usability point of view the scheme is user friendly and takes very less time for login. The proposed methodology shows significant low error rate during login procedure. In future we will explore how to extend this scheme for fully observable attacker model.

REFERENCES

1. M.M. Group, http://www.internetworldstats.com/stats.htm,June2012.searchsecurity.techtarget.com/definition/man-in-the-middle-attack(last access october, 2013).
2. C. Herley, P. C. Oorschot, and A. S. Patrick, Passwords: If were so smart, why are we still using them?, in Financial Cryptography,pp.,2009.
3. H. Tao and C. Adams, Pass-Go: A proposal to improve the usability of graphical passwords, International Journal of Network Security, vol. 7,no. 2, pp.273292, 2008.
4. T.Perkovic, M. Cagalj, and N.Saxena, Shouldr-surng safe login in a partially observable attacker model, in Sion, R.(eds.) FC 2010. LNCS, pp. 351358,2010.